Method for mutual authentication and cryptographic key agreement

Patent number:	CN1249587
Publication date:	2000-04-05
Inventor:	PATEL SAVA (US)
Applicant:	LUCENT TECHNOLOGIES INC (US)
Classification:	
- international:	H04L9/14; H04L29/06; H04Q7/20
- european:	H04L29/06C6C2; H04Q7/38A
Application number:	CN19990110264 19990729
Priority number(s):	US19980127767 19980731

Also published as:

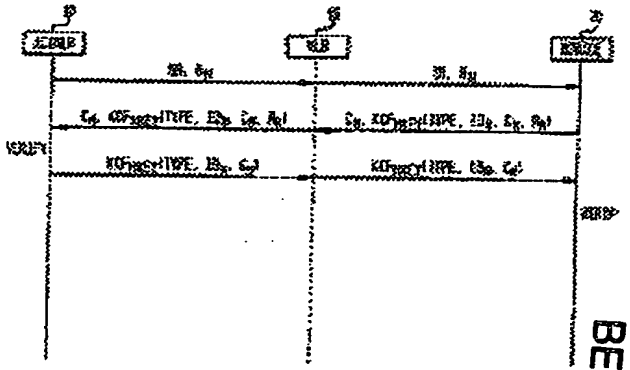
EP0998095 (A2)
JP2000106553 (A
EP0998095 (A3)
CA2277761 (A1)
EP0998095 (B1)

more >>

Abstract not available for CN1249587
Abstract of corresponding document: **EP0998095**

According to the two party authentication method, a first party generates and transfers a random number to a second party as a first challenge. The second party increments a count value in response to the first challenge, generates a first challenge response by performing a keyed cryptographic function (KCF) on the first challenge and the count value using a first key, and transfers the count value, as a second challenge, and the first challenge response to the first party. The first party verifies the second party based on the first challenge, the second challenge and the first challenge response. The first party also generates a second challenge response by performing the KCF on the second challenge using the first key, and transfers the second challenge response to the second party. The second party verifies the first party based on the second challenge and the second challenge response. For instance, the first and second parties can be a network and mobile, respectively, in a wireless system. Also, based on the first and second challenges, both the first and second parties may generate another key.

FIG. 3



[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
H04L 9/14
H04L 29/06 H04Q 7/20

[12]发明专利申请公开说明书

[21]申请号 99110264.9

[43]公开日 2000年4月5日

[11]公开号 CN 1249587A

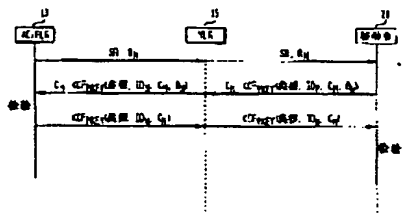
[22]申请日 1999.7.29 [21]申请号 99110264.9
[30]优先权
[32]1998.7.31 [33]US [31]09/127,767
[71]申请人 朗迅科技公司
地址 美国新泽西
[72]发明人 萨瓦·帕特尔
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 罗亚川

权利要求书3页 说明书7页 附图页数2页

[54]发明名称 双方认证和密钥协定的方法

[57]摘要

按照认证方法,第一方产生和传送一个随机数到第二方作为第 一询问。第二方响应第一询问将计数值加1,利用第一密钥通过对第 一询问和计数值执行加密钥的密码函数(KCF)运算产生第一询问 响应和传送作为第二询问的计数值和第一询问响应到第一方。第一 方基于第一询问、第二询问和第一询问响应检验第二方。第一方利 用第一密钥通过对第二询问执行 KCF 运算产生第二询问响应和传送 第二询问响应到第二方。第二方基于第二询问和第二询问响应检验 第一方。



ISSN1008-4274

99.07.29

权 利 要 求 书

1.一种在第二方认证第一方的方法，包括：

（a）从所述第一方接收一个随机数作为第一询问；

（b）响应于所述第一询问的接收对计数值加 1；

（c）利用第一密钥通过对所述第一询问和所述计数值执行加密钥的密码函数（KCF）运算产生第一询问响应；

（d）传送作为第二询问的所述计数值，所述第一询问响应所述第一方；

（e）从所述第一方接收第二询问响应，所述第二询问响应是利用所述第一密钥对所述第二询问执行所述 KCF 的结果；和

（f）基于所述第二询问和所述第二询问响应检验第一方。

2.权利要求 1 的方法，在所述步骤（c）之前还包括：

（g）利用一个根密钥产生所述第一密钥。

3.权利要求 1 的方法，其中所述步骤（c）通过利用所述第一密钥对所述第一询问、所述计数值、和用于第二方的识别符执行所述 KCF 运算来产生所述第一询问响应。

4.权利要求 1 的方法，还包括：

（g）基于所述第一和第二询问建立第二密钥。

5.权利要求 1 的方法，其中所述步骤（a）从所述第一方接收一个全局询问作为所述第一询问。

6.权利要求 1 的方法，其中所述第一方是无线系统的网络和所述第二方是移动台。

7.权利要求 6 的方法，其中所述步骤（c）通过利用所述第一密钥对所述第一询问、所述计数值和类型数据执行所述 KCF 运算来产生所述第一询问响应，所述类型数据指示由所述网络和所述移动台执行的协议的类型。

8.权利要求 6 的方法，其中所述步骤（c）通过利用所述第一密钥对所述第一询问、所述计数值、所述用于所述移动台的识别符和

类型数据执行所述 KCF 运算产生所述第一询问响应，所述类型数据指示由网络和所述移动台执行的协议的类型。

9.权利要求 6 的方法，还包括：

（g）基于所述第一和第二询问建立第二密钥。

10.权利要求 9 的方法，其中所述第二密钥是加密共享数据和对话密钥之一。

11.权利要求 6 的方法，其中所述步骤（b）利用大于 64 比特的比特计数器加 1 所述计数值和该计数器是利用一个随机数初始化的。

12.一种在第二方认证第一方的方法，包括：

（a）输出一个随机数作为第一询问；

（b）从所述第一方接收第二询问和第一询问响应，所述第二询问是一个计数器值，和所述第一询问响应是利用第一密钥对所述第一询问和所述计数值执行加密钥的密码函数（KCF）的结果；和

（e）基于所述第一询问、所述第二询问、和所述第一询问响应检验所述第一方。

13.权利要求 12 的方法，还包括：

（f）基于所述第一和第二询问建立一个第二密钥。

14.权利要求 12 的方法，其中所述步骤（a）输出所述第一询问作为一个全局询问。

15.权利要求 12 的方法，其中所述第一方是无线系统的移动台和所述第二方是网络。

16.权利要求 15 的方法，还包括：

（f）基于所述第一和第二询问建立一个第二密钥。

17.权利要求 16 的方法，其中所述第二密钥是加密共享数据和对话密钥之一。

18.权利要求 12 的方法，还包括：

（f)利用所述第一密钥通过对所述第二询问执行所述 KCF 运算来产生第二询问响应；和

（g）传送所述第二询问响应到所述第二方。

19.权利要求 18 的方法，其中所述步骤（f）利用所述第一密钥通过对所述第二询问和用于所述第二方的识别符执行所述KCF运算来产生所述第二询问响应。

20.权利要求 18 的方法，其中所述第一方是无线系统的移动台和所述第二方是网络。

21.权利要求 20 的方法，其中所述步骤（f）通过利用所述第一密钥对所述第二询问和类型数据执行所述KCF运算来产生所述第二询问响应，所述类型数据指示由网络和所述移动台执行的协议的类型。

22.权利要求 20 的方法，其中所述步骤（f）通过利用所述第一密钥对所述第二询问、用于所述网络的识别符和类型数据执行所述KCF运算来产生所述第二询问响应，所述类型数据指示由网络和所述移动台执行的协议的类型。

说　明　书

双方认证和密钥协定的方法

与本申请同时提交的下列各申请是与本申请的主题相关的，并以这些申请的整体援引于此以资参考，这些申请是：发明人为本申请的发明人、申请号未定的、名称为 METHOD FOR UPDATING SECRET SHARED DATA IN A WIRELESS COMMUNICATION SYSTEM 的申请；发明人为本申请的发明人、申请号未定的、名称为 METHOD FOR TRANSFERRING SENSITIVE INFORMATION USING INTIALLY UNSECURED COMMUNICATION 的申请；发明人为本申请的发明人、申请号未定的、名称为 METHOD FOR SECURING OVER-AIR- COMMUNICATION IN A WIRELESS SYSTEM 的申请；和发明人为本申请的发明人和 Adam Berenzweig、申请号未定的、名称为 METHOD FOR ESTABLISHING A KEY USING OVER-THE-AIR COMMUNICATION AND PASSWORD PROTOCOL AND PASSWORD PROTOCOL 的申请。

本发明涉及一种用于认证一些通信方与另外一方的方法，和在一个申请中，用于认证在无线通信中的一个移动台和一个网络的方法。本发明还涉及基于该认证协议的密钥协定。

用于认证一些通信方与另外一方的协议提供了对通信保密的一种度量。由无线通信工业使用着若干种这样的协议和在美国、欧洲和日本形成了不同通信标准的部分。

虽然按照本发明的通信用户认证系统和方法并不限于无线通信，但为了使容易理解，在说明书中本发明将按无线系统进行描述。为此，提供一个无线系统的一般概况，包括对使用至少各标准之一的通信用户认证协议的讨论。

当前美国利用具有不同标准的三种主要无线系统。第一个系统

是时分多址系统（TDMA）并且按照 IS-136 标准；第二个系统是符合 IS-95 标准的码分多址系统（CDMA）；和第三个系统是高级移动电话系统（AMPS）。所有这三个系统利用 IS-41 标准作系统之间交换消息，该标准为始发呼叫、更新加密共享数据等等限定认证程序。

图 1 表示包括认证中心（AC）、原始位置寄存器（HLR）10、正在访问位置寄存器（VLR）15 和移动台 20 的无线系统。虽然多于一个的 HLR 可以与 AC 相关联，但现在是一一对应的情况。因此，图 1 表示 HLR 和 AC 作为一个单一的实体，虽然它们是可以分开的。另外，为了简化起见，本说明书的下面部分将 HLR 和 AC 结合在一起称为 AC/ HLR。再有，VLR 发送信息到与之相关的多个移动交换中心（MSC）之一，和每个 MSC 发送信息到多个基站（BS）之一，以便发送到移动台。为了简单起见，VLR、MSC 和 BS 都被称为和表示为 VLR。总的说来，由网络提供商进行操作的 AC、HLR、VLR、MSC 和 BS 被称为网络。

公知为 A 密钥的根密钥仅被存储在 AC/ HLR 10 和移动台 20 中。还有公知的共享加密数据 SSD 的二次密钥，该密钥随着该移动台漫游（即，当该移动台到它的原始覆盖之外时）被发送到 VLR 15。SSD 是利用密码算法或函数从 A 密钥和随机数种子密钥 RANDSSD 产生的。密码函数是一种函数，它基于可能的输入范围产生具有预定比特数的输出。加密钥的密码函数（KCF）是基于一个密钥进行运算的一种类型的密码函数。例如，一个密码函数工作在两个或多个自变量（即，输入），其中一个自变量是密钥。来自正在利用的 KCF 的输出和情报，各输入可以是不确定的，除非该密钥是已知的。各种加密/解密算法是各密码函数的类型。如伪随机函数（PRF)和消息认证码（MAC）的各单方向函数也是如此。表达式 $KCF_{SK}(R_N')$ 代表利用对话密钥 SK 作为密钥的随机数 R_N' 的 KCF。对话密钥是一种持续一段对话的密钥，和一段对话是诸如一次呼叫长度的时间周期。

在 IS-41 协议中，所用的密码函数是 CAVE（蜂窝式认证和话音

加密）。当移动台 20 漫游时，在该区的 VLR15 发一个认证请求到 AC/ HLR 10，AC/ HLR 10 通过发送该移动台的 SSD 进行响应。一旦 VLR15 具有 SSD，它可以独立于 AC/ HLR 10 认证移动台 20。为了保密的缘故，SSD 该周期性地进行更新。

图 2 表示 AC/ HLR 10、VLR15 和移动台 20 之间的通信以更新 SSD。如上所述，AC/ HLR 10 产生一个随机数种子密钥 RANDSSD，和利用 CAVE 算法产生利用该随机数种子密钥 RANDSSD 的新的 SSD。该 SSD 为 128 比特长。第一 64 比特用作第一 SSD，叫做 SSDA，和第二 64 比特用作第二 SSD，叫做 SSDB。如图 2 所示，AC/ HLR 10 提供给 VLR15 以新的 SSD 和 RANDSSD。然后，VLR15 随着对话请求 SR 发送 RANDSSD 到移动台 20。对话请求 SR 指示移动台 20 执行该 SSD 协议，这在下面详细描述。响应于 RANDSSD 和对话请求 SR 的接收，移动台 20 利用 CAVE 算法和利用该 RANDSSD 产生新的 SSD，和利用随机数发生器产生随机数 R_M。移动台 20 发送随机数 R_M 到 VLR15。移动台 20 还利用新的 SSDA 作为密钥对随机数 R_M 执行 CAVE 算法。这种计算由 $CAVE_{SSDA}(R_M)$ 表示。

VLR15 和 AC/ HLR 10 之一还计算 $CAVE_{SSDA}(R_M)$，和发送其结果到移动台 20。如果计算的 $CAVE_{SSDA}(R_M)$ 与从网络接收的相匹配，则移动台 20 认证该网络。

接下来，和一般在从指示核实的移动台 20 接收信号之后，VLR15 产生一个随机数 R_N，发送这个随机数 R_N 到移动台 20。同时，VLR 计算 $CAVE_{SSDA}(R_N)$。当收到 R_N 后，移动台 20 计算 $CAVE_{SSDA}(R_N)$，和发送结果到 VLR15。VLR15 认证移动台，看是否它计算的 $CAVE_{SSDA}(R_N)$ 与从移动台 29 接收的相匹配。随机数 R_M 和 R_N 被称为询问（challenge），而 $CAVE_{SSDA}(R_M)$ 和 $CAVE_{SSDA}(R_N)$ 被称为应答。一旦认证完成，移动台 20 和网络利用 SSDB 产生对话密钥。

在这种协议中，SSD 本身被用于应答来自移动台 20 和网络的询问。当老的 RANDSSD 和 SSD 对被展现时，这可以考虑到一种攻击。

知道这个对足以询问移动台 20，和应答它的询问。因此，一个攻击者可以发 SSD 的更新到移动台 20，和应答来自移动台的询问。一旦所展现的 SSD 是可接受的，和尽管一个加密对话密钥协定协议（即，在移动台和网络之间通信建立一种对话密钥的协议），攻击者可以在欺诈识别下假冒该网络和发一个呼叫到移动台 20。例如，该假冒者可以输入他自己的主叫用户 ID 或姓名和假装是某其它人。该攻击者可以假装是一个信用卡公司，和询问检验卡号和个人识别号。或甚至在主叫用户名称栏中使用电话公司的名称和询问检验主叫卡号，等等。

在按照本发明的两个用户认证的方法中，第一方发送一个随机数作为第一询问。第二方利用第一询问响应来响应。第一询问响应是通过对第一询问和利用第一密钥的计数值执行加密钥的密码函数（KCF）运算产生的。当收到第一询问时，第二方对计数值加 1，和利用该计数值作为第二询问。第一方基于第一询问和第二询问的接收和第一询问响应来检验第二方。在检验以后，第一方利用第一密钥对第二询问执行 KFC 运算，产生第二询问响应。基于第二响应和第二询问响应的接收，第二方检验第一方。利用第一和第二询问，由双方产生一个加密密钥。按这种方式，作为与加密密钥不同的密钥，第一密钥被使用在应答各询问中。本发明具有许多应用，包括其中第一和第二方分别是网络和移动台的无线通信工业。

从下面给出的详细描述和附图中，将使本发明变得更容易理解，这些附图仅是以说明的方式给出的，在各个附图中相同的标号在各不同的附图中代表对应的部件，和其中：

图 1 是说明一个无线系统的基本部分的框图；

图 2 表示按照 IS-41 标准更新加密共享数据在认证中心/原位位置寄存器、正在访问位置寄存器、和移动台之间的通信；

图 3 表示按照本发明的一个实施例的认证双方的在网络和移动台之间的通信。

正如上面所讨论的，虽然按照本发明的用户认证系统和方法并

不是限制在无线通信中，但为了容易理解，本发明将按无线系统的角度进行描述。更为具体地，按照本发明的双方认证的方法或协议将按照使用如图 1 所示的无线系统进行描述的。

与上面相对于图 1 和 2 所讨论的方法或协议相比，在按照本发明的方法中，AC/ HLR 10 和移动台 20 基于 A 密钥还产生称为 M 密钥的另一种密钥。例如，M 密钥是通过对网络 10 和移动台 20 都知道的值施加由 A 密钥索引的伪随机函数（PRF）产生的。一种具体的 PRF 是来自 NIST（国家标准协会）的公知的数据加密标准密码码块链（DES-CBC）（Data Encryption Standar-Cipher Block Chaining）算法。在一个优选实施例中，对一个已知值施加由 64 比特 A 密钥索引的 DES-CBC，产生一个 64 比特 M 密钥。

图 3 表示按照本发明的一个实施例认证双方用户的在网络和移动台 20 之间的通信。如所示，VLR15 起到在 AC/ HLR 10 和移动台 20 之间通信的渠道的作用。更具体地，按照本发明的认证协议是在 AC 和移动台 20 之间执行的。

如所示，一方、AC/ HLR 10 产生和发送一个随机数 R_N 到另一方移动台 20。一般地，AC/ HLR 10 除了发送随机数 R_N 外，还发送规定将被执行的协议类型的对话请求 SR。协议类型包括，例如，呼叫始发、加密的共享数据（SSD）更新、呼叫结束、和移动台登记。

作为响应，移动台 20 产生计数值 C_M，和利用 M 密钥作为密钥，对随机数 R_N、计数值 C_M、类型数据、id 数据 ID_M 执行 KCF 运算。这种计算由 $KCF_{M\text{-}Key}$（类型、ID_M、C_M、R_N）代表。最好是，KCF 是诸如 HMAC 之类的加密钥的消息认证码，但也可以是诸如 DES-CBC 之类的 PRF。移动台 20 包括产生计数值 C_M 的计数器。移动台 20 在产生询问响应（即，$KCF_{M\text{-}Key}$（类型、ID_M、C_M、R_N））之前对每个来自网络的询问对计数值 C_M 加 1。

类型数据代表被执行的协议的类型。id 数据指示从移动台发出的通信。一般 id 数据 1 指示通信是来自网络的，和 id 数据 0 指示通信是来自移动台的。但是，为了讨论的目的，对于移动台 20 的 id

数据被表示为 ID_M 和对于网络的 id 数据被表示为 ID_N。当对随机数 R_N 和计数值 C_M 执行 KCF 运算时对于双方用户认证的系统和方法不要求包括类型数据。类型数据和具体的 id 数据已经被包括作为对于无线系统双方认证的系统和方法的应用的一部分。

移动台 20 发送计数值 C_M 和 $KCF_{M\text{-}Key}$（类型、ID_M、C_M、R_N）到网络。因为 AC/ HLR 10 启动包括按照本发明的双方认证协议的当前协议，AC/ HLR 10 知道类型数据。另外，因为来自移动台的通信包括相同的 id 数据，这个值也是 AC/ HLR 10 知道的。因此，基于接收的计数值 C_M，AC/ HLR 10 计算 $KCF_{M\text{-}Key}$（类型、ID_M、C_M、R_N）和确定是否所计算的值与从移动台 20 接收的版本匹配。如果发现匹配，则 AC/ HLR 10 认证该移动台 20 。

一旦移动台 20 已经被检验，AC/ HLR 10 计算 $KCF_{M\text{-}Key}$（类型、ID_N、C_M），和发送计算的结果到移动台 20。同时，移动台 20 也计算 $KCF_{M\text{-}Key}$（类型、ID_N、C_M）。然后，移动台 20 检验是否所计算的 $KCF_{M\text{-}Key}$（类型、ID_N、C_M）版本与从 AC/ HLR 10 接收的版本匹配。如果发现匹配，则移动台 20 认证该网络。

另外，在执行这种双方认证协议后，可以产生其它密钥。例如，如果图 1 的无线系统使用这种双方认证协议作为 SSD 更新协议，则移动台 20 认证网络后，移动台 20 和 AC/ HLR 10 两者具有随机数 R_N 和计数值 C_M。移动台 20 和 AC/ HLR 10 两者产生 SSD 作为 $PRF_{A\text{-}Key}$（C_M、R_N），其中 PRF 最好是 DES-CBC 算法。另外一种情况下，在其它协议中，利用相同的技术产生其它密钥。

当应用到无线系统中时，移动台 20 需要在半永久存储器中存储计数值 C_M，使得该期间功耗下降，计数值 C_M 不被重新初始化。这种方法防止计数值的重复，而计数值的重复使得攻击者在他的攻击中占优势。在一个优选的实施例中，计数值利用一个随机数被初始化和利用诸如 64 到 75 比特计数器之类的大比特计数器产生。即使当移动台 20 破坏和丢失所存储的计数值，这也提供了保密性。即使攻击者可以任意使移动台破坏，和假设他需要至少一秒时间开始对

话，当使用75比特计数器时，则在该攻击者控制移动台重复的一个计数值前，他将需要例如一年的时间。

作为另外一个替代方案，代替发送唯一随机数 R_N，开始方（例如，网络）发一个全局随机数。即，代替在图 3 的实施例中，对于每个通信开始方发不同的唯一随机数 R_N。但是，在这个替代方案中，开始方对于每个通信发相同的随机数 R_N。

在按照本发明的协议中，以前建立在各方之间的密钥（例如，A密钥或 SSD）不被用于应答询问，和因此相对于 IS41 所讨论的网络假冒问题是不可能的。另外，即使 M 密钥被展现给攻击者，则也没有直接的方法从中获得 A 密钥，因为单方向函数被用于产生 M 密钥。当发起一个攻击时，攻击者使用了以前的询问和询问响应，如果使用按照本发明的协议，这样的攻击将是要失败的。原因是这个攻击者将利用基于老的计数值的询问响应。因此，网络将不检验该攻击者。再有，在按照上面讨论的认证后产生的密钥将是利用 A 密钥通过新的询问的 PRF 产生的，和该攻击者不知道 A 密钥。

因此本发明已经进行了描述，显然本发明将利用作出按许多方法进行改变。这些改变并不被视为脱离了本发明的精神和范围，和所有这些修改都将被包括在下列权利要求书的范围内。

图 1
（现有技术）

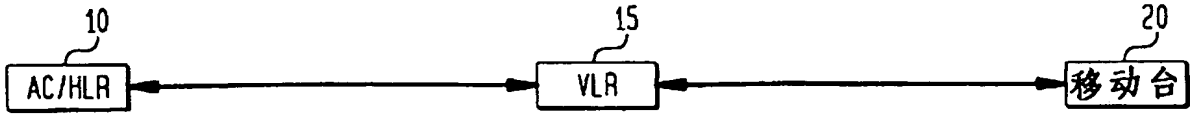


图 2
（现有技术）

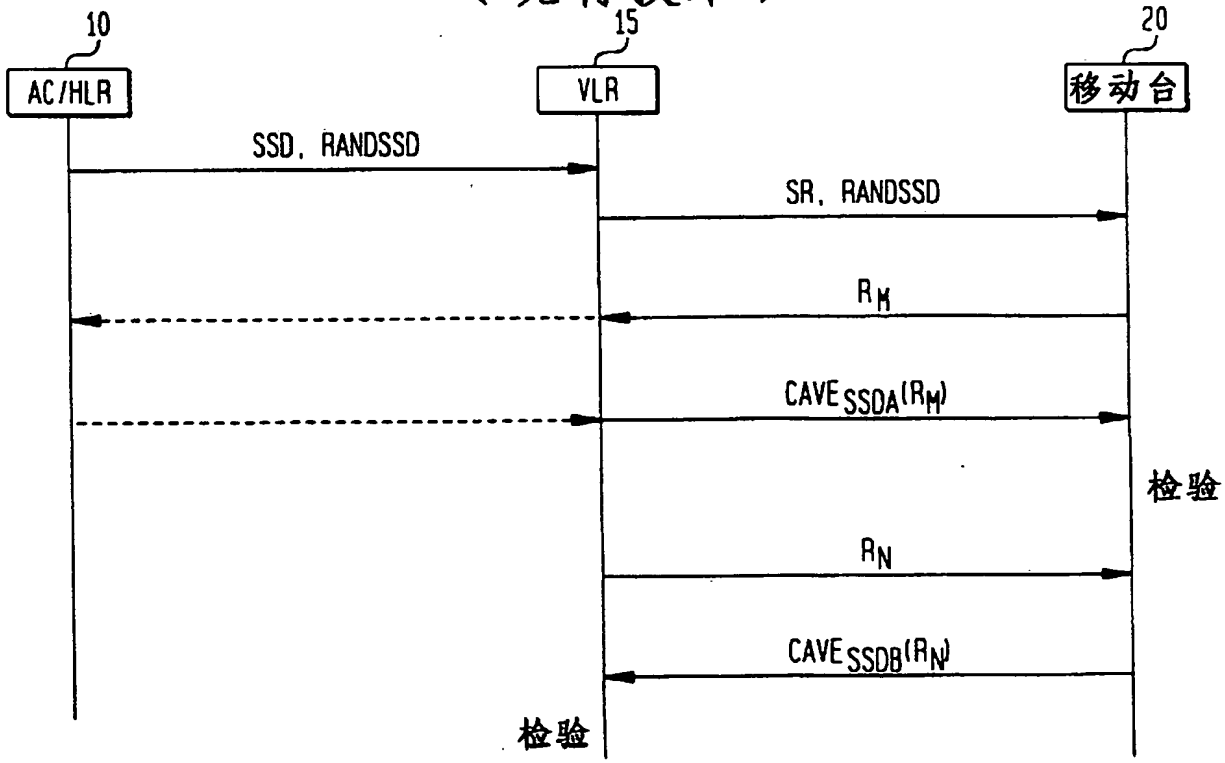
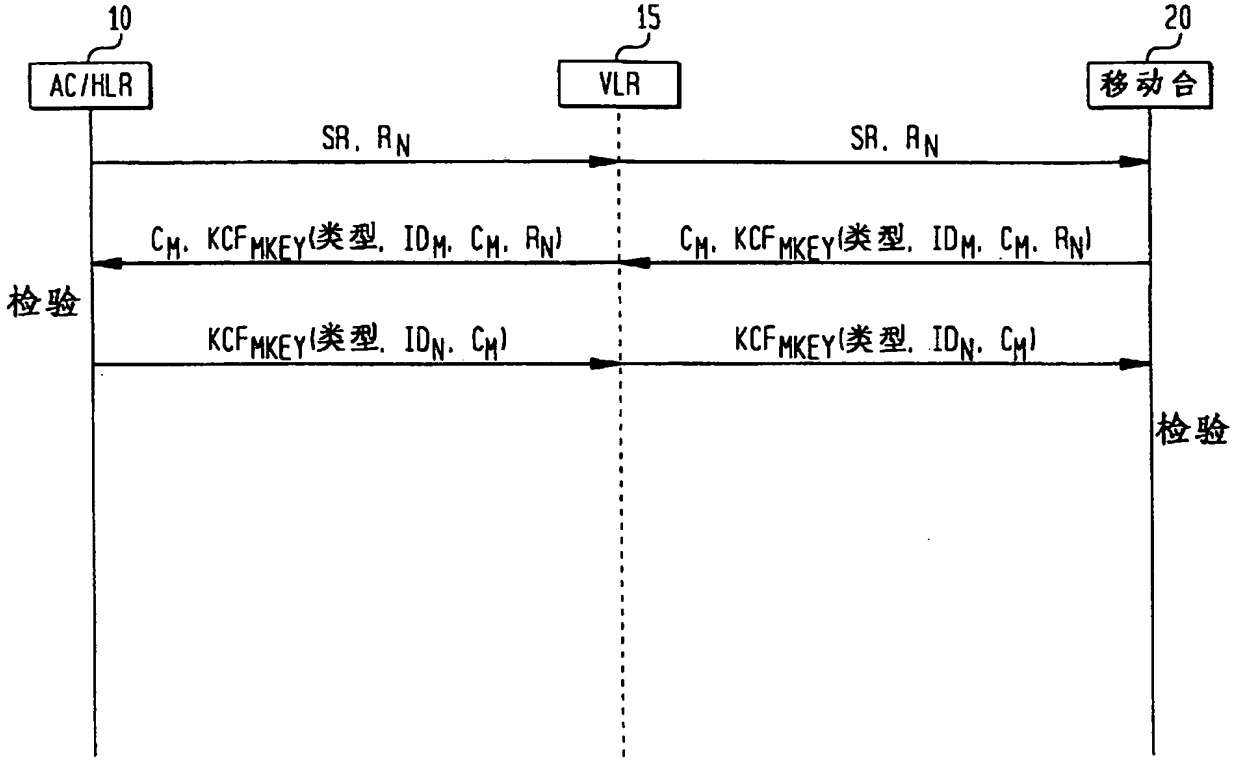


图 3


10
AC/HLR
15
VLR
20
移动台
SR, R_N
SR, R_N
C_M, KCF_{MKEY}(类型, ID_M, C_M, R_N)
C_M, KCF_{MKEY}(类型, ID_M, C_M, R_N)
检验
KCF_{MKEY}(类型, ID_N, C_M)
KCF_{MKEY}(类型, ID_N, C_M)
检验